REMARKS

I. Initial Remarks

Claims 1-20 and 25-32 are pending. Claims 1, 6, 11, and 16 are in independent form. Claims 1, 6, 11, 16-20, and 31-32 are amended, while no claims are added or cancelled. Support for the amendments may be found in the specification at least in, but not limited to, paragraphs 32, 48, and 99. For at least the following reasons, all claims are in condition for allowance.

In the Office Action, claims 16-20 and 31-32 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Claims 16-20 and 31-32 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Claims 1-20 and 25-32 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Pat. No. 5,548,646 to Aziz et al. ("Aziz"). The Office Action presents new grounds of rejection. Applicants respectfully traverse the rejections.

In view of the following arguments, all claims are believed to be in condition for allowance over the references of record. Therefore, this response is believed to be a complete response to the Office Action.[1] Further, for any instances in which the Examiner took Official Notice in the Office Action, Applicants expressly do not acquiesce to the taking of Official Notice, and respectfully request that the Examiner provide an affidavit to support the Official Notice taken in the next Office Action, as required by 37 CFR 1.104(d)(2) and MPEP § 2144.03.

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

II. Claim Rejections – 35 U.S.C. § 112

The Examiner rejected independent claim 16 and claims 17-20 and 31-32 that depend therefrom under Section 112, second paragraph, as allegedly being indefinite. Specifically, the Examiner stated that:

> While the preamble of independent claim 16 and dependent claims 17-20 and 31-32 each call for a device/apparatus, no specific hardware is recited in the body of these claims and as such, the scope of the apparatus claim is unclear.

(Office Action, page 2.) Applicants respectfully disagree with the Examiner's interpretation of definite subject matter under Section 112 paragraph 2. Applicants further submit that independent claim 16 recited definite subject matter as previously presented. However, to be even more clear regarding the recited subject matter, independent claim 16 has been amended to recite in part "[a] bastion host comprising at least one computing device adapted for processing packet header information of a data packet, the bastion host being configured to" perform the recited details. (Emphasis added.) Moreover, claims 17-20 and 21-31 are also amended to clarify that they recite additional details of how the bastion host is "further configured."

Accordingly, Applicants have clarified the scope of these pending apparatus claims, fully addressing the Examiner's rejections regarding Section 112 second paragraph. Therefore, the Section 112 second paragraph rejections of claims 16-20 and 31-32 should be reconsidered and withdrawn.

III. Claim Rejections – 35 U.S.C. § 101

The Examiner rejected claims 16-20 and 31-32 under Section 101 as allegedly being directed to non-statutory subject matter. Specifically, the Examiner stated that:

> The functions of these claims may be implemented entirely by software. Furthermore, the claims fail to define any structural or functional interrelationship between the software and the apparatus of the preamble which would permit the software's functionality to be realized.

(Office Action, page 3.) Applicants respectfully disagree with the Examiner's interpretation of statutory subject matter under Section 101. Applicants further submit that independent claim 16 was directed to statutory subject matter as previously presented. However, to facilitate prosecution and to address the Examiner's concerns, claim 16 has been amended. As indicated above, amended claim 16 now recites "[a] bastion host comprising at least one computing device adapted for processing packet header information of a data packet, the bastion host being configured to" perform the recited details. (Emphasis added.) As amended, independent claim 16 makes clearer that the "bastion host" comprises hardware, namely "at least one computing device," and that the "bastion host comprising at least one computing device" is configured as recited by claim 16.

Accordingly, independent claim 16 and claims 17-20 and 31-32 that depend therefrom recite statutory subject matter under Section 101. Thus, for at least the reasons stated above, the Examiner's Section 101 rejections have been fully addressed and should be withdrawn.

IV. Claim Rejections – 35 U.S.C. § 102

A. Independent Claim 1

Independent claim 1 was rejected under Section 102(b) as allegedly being anticipated by Aziz. As amended, independent claim 1 recites in part:

> a translator configured to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated, and placed back into the packet header information of the data packet.

Before amendment, the Examiner rejected the aforementioned recitation over the Abstract, column 6 lines 1-11, and column 7 lines 55-65 of Aziz. (Office Action, pages 3-4.) Aziz is a newly cited reference that discloses a "tunnelling bridge" used to encapsulate and transmit a packet with an "appended" "encapsulation header," where the "encapsulation header" is then used to decrypt the

encapsulated packet. (E.g., Aziz, Abstract; col. 5, lines 48-55.) Thus, while Aziz discloses to decrypt an encapsulated packet using information retrieved from an appended encapsulation header, Aziz does not disclose or suggest "a translator configured to restore predetermined portions of packet header information of a data packet" at all, let alone "the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated, and placed back into the packet header information of the data packet" as recited in the context of independent claim 1. Accordingly, for at least these reasons independent claim 1 is patentable over Aziz.

Aziz discloses "[a] system for automatically encrypting and decrypting data packet sent from a source host to a destination host across a public internetwork." (Aziz, Abstract.) In Aziz, "[a] tunnelling bridge is positioned at each network, and intercepts all packets transmitted to or from its associated network." (Id.) When it is determined that a packet "transmitted from a first host . . . should be encrypted, . . . the packet is encrypted, and transmitted to the destination network along with an encapsulation header indicating source and destination information: either source and destination host addresses, or the broadcast addresses of the source and destination networks." (Id.; Emphasis added.) With regard to the encryption, Aziz further explains that:

> The data structure 402 for mode 1 is represented in FIG. 8. The original data 410 and original header 420 are now encrypted, indicated as (410) and (420). Encryption key management information 440 is appended (in encrypted form) as pan [sic] of the new encapsulation header 430, along with a new IP header 450, including the addresses of the source and destination hosts. The information 430 includes [sic] indicates which encryption scheme was used.

(Aziz, col. 5, lines 48-55; Emphasis added.)

Then, "[at] the destination network, the associated tunneling bridge intercepts the packet, inspects the encapsulation header, from an internal table determines whether the packet was encrypted, and from either the source (host or network) address or the tunnelling bridge identifier determines whether and how the packet was encrypted." (Aziz, Abstract.) Further, "[if] the packet was encrypted, it is now decrypted using a key stored in the destination tunnelling bridge's memory,

and is sent on to the destination host." (Id.; Emphasis added.) Accordingly, Aziz discloses to encrypt a packet, add an encapsulation header to the packet, transmit the packet, inspect the encapsulation header, and use the encapsulation header to decrypt the encapsulated packet.

However, Aziz does not teach or suggest "a translator configured to restore predetermined portions of packet header information of a data packet" as recited in the context of independent claim 1. In contrast, Aziz discloses that "[if] the packet was encrypted, it is now decrypted," indicating that the entire encapsulated packet is decrypted, without regard to any "predetermined portions of packet header information of a data packet." (Aziz, Abstract.)

Moreover, Aziz discloses to "[inspect] the encapsulation header," and "[if] the packet was encrypted, it is now decrypted using a key stored in the destination tunnelling bridge's memory." However, wholesale decryption of an encapsulated packet simply does not teach or suggest "the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated, and placed back into the packet header information of the data packet." (Emphasis added.) Further, Aziz apparently discards the encapsulation header once the encapsulated packet is decrypted, and thus the encapsulation header additionally fails to teach or suggest "the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated, and placed back into the packet header information of the data packet" as recited in the context of independent claim 1.

Accordingly, for at least these reasons, independent claim 1 and all claims that depend therefrom are patentable over Aziz.

B. Independent Claims 6, 11, And 16

Each of independent claims 1, 6, 11, and 16 was rejected under Section 102(b) as allegedly being anticipated by Aziz. While claims 1, 6, 11, and 16 are each of different scope, for at least

reasons similar to those discussed above with regard to independent claim 1, independent claims 6, 11, and 16 are patentable over Aziz.

For example, as discussed above with regard to independent claim 1, Aziz does not teach or suggest:

> . . . to restore predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include a previously translated address, the previously translated address being extracted from the packet header, restored into an address from which the previously translated address was translated, and placed back into the packet header of the data packet.

Independent claims 6, 11, and 16 each include a like recitation, although claim 6 recites "restoring," claim 11 recites "means for restoring," and claim 16 recites to "restore."

Accordingly, for at least similar reasons to those discussed above with regard to independent claim 1, independent claims 6, 11, and 16 and all claims that depend therefrom are patentable over Aziz.

C. Dependent Claims 2-5, 7-10, 12-15, And 25-32

Claims 2-5, 7-10, 12-15, and 25-32 are in condition for allowance at least because they depend from one of independent claims 1, 6, 11, or 16. Further, the dependent claims also recite independently patentable subject matter, representative examples of which are discussed below.

1. Claim 2, 7, 12, And 17

Claim 2 depends from independent claim 1 and recites in part "wherein the security device is a logging device configured to log the data packet." The Examiner cited col. 7, lines 49-54 of Aziz as allegedly disclosing the recitation. (Office Action, page 4.) The cited portion of Aziz states:

> An alternative to the use of hosts or networks tables in the memories of the source and destination tunnelling bridges (or source and destination hosts, as the case may be) would be any information

> identifying one or more predetermined criteria by which the source host or source tunnelling bridge determines whether to encrypt a given data packet. Such criteria need not merely be source and destination information, but could include packet contents, time of transmission, subject header information, user id., presence of a key word (such as "encrypt") in the body of the packet, or other criteria.

(Aziz, col. 4, lines 49-54.) However, disclosure of an alternative method of determining whether to encrypt a given data packet bears no relation to a "logging device configured to log the data packet," let alone "wherein the security device is a logging device configured to log the data packet" as recited in the context of claim 2.

Moreover, the cited portion of Aziz further fails to teach or suggest the recitations of claim 2 when claim 2 is considered in the context of independent claim 1. Claim 1 recites in part "an actuator configured to trigger a security device when the address does not match an entry in the host table," while claim 2 further recites "wherein the security device is a logging device configured to log the data packet" (Emphasis added.) The cited paragraph of Aziz discusses use of the "tunneling bridge" with "predetermined criteria" as "[an] alternative to the use of hosts or networks tables." (Aziz, col. 4, lines 49-54; Emphasis added.) Clearly, as the cited paragraph of Aziz discloses alternatives to use of "hosts or network tables," the cited portion of Aziz does not teach or suggest "an actuator configured to trigger a security device when the address does not match an entry in the host table," "wherein the security device is a logging device configured to log the data packet" as recited in the context of the claim.

For at least these reasons, claim 2 is separately patentable over Aziz.

Moreover, claim 7 recites in part "logging the data packet when the address does not match an entry in the host table." (Emphasis added.) Claim 12 recites in part "means for logging the data packet when the address does not match an entry in the host table." Claim 17 recites in part "the bastion host being further operable to log the data packet when the address does not match an entry in the host table." (Emphasis added.) The Examiner indicated that these claims are rejected according to the previous rejections of claims 1-5 and 25-26. (Office Action, page 5.) However, for

reasons similar to those discussed above with regard to claim 2, Aziz lacks the requisite disclosure. Thus, for at least reasons similar to those discussed above with regard to claim 2, claims 7, 12, and 17 are separately patentable.

2. Claims 3, 8, 13, And 18

Claim 3 recites in part "wherein the security device is configured to signal an alarm when triggered." The Examiner cited column 15, lines 1-17 and 27-39 of Aziz as allegedly disclosing the recitation. (Office Action, page 4.) The cited sections of Aziz state as follows:

> 4.0 Management of [Diffie-Hellman (DH)] Certificates
>
> Since the nodes' public DH values are communicated in the form of certificates, the same sort of multi-tier certification structure that is being deployed for PEM [6] and also by the European PASSWORD project can be used. Namely, there can be a Top Level Certifying Authority (TLCA) which may well be the same the Internet Policy Registration Authority (IPRA), Policy Certifying Authorities (PCAs) at the second tier and organizational CAs below that. In addition to the identity certificates, which are what are part of PEM certificate infrastructure, we also need additional authorization certificates, in order to properly track the ownership of IP addresses. Since we would like to directly use IP addresses in the DH certificates, we cannot use name subordination principles alone (as e.g {sic} used by PEM) in order to determine if a particular CA has the authority to bind a particular IP address to a DH public value.
>
> …
>
> The node certificates are issued by organizational CAs which have jurisdiction over the range of IP addresses that are being certified. The PCAs will have to perform suitable checks (in line with the advertised policy of that PCA) to confirm that the organization which has jurisdiction over a range of addresses is issued a certificate giving it the authority to certify the DH values of individual nodes with those addresses. This authority will be delegated in the form of a {sic} authorization certificate signed by the PCA. For the purposes of authorization, the CA's Distinguished Name (DN) will be bound to the range of IP addresses over which it has jurisdiction. The CA has either an RSA or DSA certificate issued by the PCA.

(Aziz, col. 15, lines 1-17, 27-39.) However, disclosure of management of Diffie-Hellman certificates bears no relation to "wherein the security device is configured to signal an alarm when triggered" as recited in the context of claim 3. Accordingly, Aziz does not teach or suggest "wherein the security device is configured to signal an alarm when triggered." For at least these reasons, claim 3 is separately patentable.

Moreover, claim 8 recites in part "signaling an alarm when the security device is triggered." Claim 13 recites in part "means for signaling an alarm when the security device is triggered." Claim 18 recites in part "the bastion host being further operable to signal an alarm when the security device is triggered." The Examiner indicated that these claims are rejected according to the previous rejections of claims 1-5 and 25-26. (Office Action, page 5.) However, as discussed above with regard to claim 3, Aziz lacks the requisite disclosure. For at least reasons similar to those discussed above with regard to claim 3, claims 8, 13, and 18 are separately patentable.

3. Claims 25-32

Claim 25 recites in part "wherein the address includes a network portion and an apparatus portion, the apparatus portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the apparatus portion of the address without also restoring the network portion of the address." The Examiner cited column 2, lines 32-36, and column 6, lines 21-33 of Aziz as allegedly disclosing the recitation. (Office Action, page 5.) The cited sections of Aziz state as follows:

> If the encapsulation header utilizes the network IP source and destination addresses, with the source and destination host addresses encrypted, then the host identities are also concealed, and an intervening observer can discern only the networks' identities.
>
> ...
>
> In mode 2, a data structure 404 is used, and includes a new encapsulation header 432. It includes key encryption management information 440, which is appended to the original data packet 400, and both are encrypted, resulting in encrypted fields (410), (420) and (440) shown in FIG. 9. A new IP header 470 including the broadcast addresses of the source and destination networks (not the addresses of

> the hosts, as in field 450 in FIG. 8) is appended. In addition, a tunnelling bridge identifier field 460 is appended as part of the encapsulation header 432. Here, fields 410, 420 and 440 in this embodiment are all encrypted, while fields 460 and 470 are not.

(Aziz, col. 2, lines 32-36; col. 6, lines 21-33.) However, general disclosure regarding an "encapsulation header" and an encrypted "original packet" in no way teaches or suggests the recitations of claim 25. For example, Aziz does not teach or suggest "wherein the address includes a network portion and an apparatus portion." Moreover, Aziz does not teach or suggest "the apparatus portion of the address having been translated without the network portion also being translated," and "wherein said translator is configured to restore the apparatus portion of the address without also restoring the network portion of the address." For at least these reasons, claim 25 is separately patentable.

Moreover, claim 26 recites in part:

> wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein said translator is configured to restore at least a portion of the packet header information in the one or more predetermined fields.

The Examiner cited the same sections of Aziz (i.e., col. 2, lines 32-36; col. 6, lines 21-33) as allegedly disclosing this recitation as well. (Office Action, page 5.) However, general disclosure regarding an "encapsulation header" in no way teaches or suggests the recitations of claim 26. For example, Aziz does not teach or suggest "the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header." (Emphasis added.) For at least these reasons, claim 26 is separately patentable.

Although of different scope, claims 27, 29, and 31 each include recitations similar to those recited by claim 25. Additionally, while of different scope, claims 28, 30, and 32 each include recitations similar to those recited by claim 26. The Examiner indicated in the Office Action that claims 27-32 are rejected according to the previous rejections of claims 1-5 and 25-26. (Office Action, page 5.) However, for at least reasons similar to those discussed above with regard to claims 25 and 26, Aziz lacks the requisite disclosure. Thus, claims 27-32 are separately patentable over Aziz.

CONCLUSION

In view of the above amendment, Applicants believe the pending application is in condition for allowance. Reconsideration and allowance are respectfully requested.

It is believed that any fees associated with the filing of this paper are identified in an accompanying transmittal. However, if any additional fees are required, they may be charged to Deposit Account No. 18-0013, under Order No. 65632-0534. To the extent necessary, a petition for extension of time under 37 C.F.R. § 1.136 is hereby made, the fee for which should be charged against the aforementioned account.

Dated: July 31, 2009

Respectfully submitted,

Electronic signature: /Isaac T. Slutsky/
Isaac T. Slutsky
Registration No.: 64,620
Michael B. Stewart
Registration No.: 36,018
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 25537
Attorney for Applicant